# Vereinbarungen über ITEG-Hosting als Auftragsverarbeitung nach Art. 28 DSGVO

## Vereinbarungen über ITEG-Hosting als Auftragsverarbeitung nach Art. 28 DSGVO

Da das vielfach verwendete Muster der WKO einige problematische Details enthält stellen wir ein eigenes Muster für Vereinbarungen für Auftragsverarbeitung nach § 28 DSGVO zur Verfügung.

Falls Sie das WKO-Muster oder ein anderes Muster verwenden wollen beachten Sie bitte unbedingt unserer "Änderungen zur WKO-Vorlage" und Anmerkungen im übernächsten Kapitel.

### ITEG-Muster für Vereinbarungen über ITEG-Hosting als Auftragsverarbeitung

Die Bearbeitung unserer Vorlagen durch Kunden hat sich als Fatal für das Layout erwiesen. Wir bitten daher um Download des Musters als PDF und um Bekanntgabe aller "auszufüllenden" Daten, wir schicken dann umgehend ein ausgefülltes PDF retour.

| Version, Veröffentlichungsdatum | Änderung(en) | Download als PDF |
|---|---|---|
| veraltet: 1.0 vom 7.5.2018 | | ~~Auftragsverarbeitungs-Vereinbarung_ITEG-Muster_1.0.pdf~~ (bzw. ~~odt~~ und ~~docx~~) |
| veraltet: 1.1 vom 23.5.2018 | | ~~Auftragsverarbeitungs-Vereinbarung_ITEG-Muster_1.1.pdf~~ |
| veraltet: 1.2 vom 24.5.2018 | | ~~Auftragsverarbeitungs-Vereinbarung_ITEG-Muster_1.2.pdf~~ |
| veraltet: 1.2.1 v. 5.5.2020 | 1 Copy/Paste-Fehler korrigiert | - |
| **aktuell: 1.2.2 v. 21.6.2021** | Büro-Adresse, Liste Housing-Anbieter | **Auftragsverarbeitungs-Vereinbarung_ITEG-Muster_1.2.2.pdf** |

### Technische und Organisatorische Maßnahmen (TOMs) der ITEG IT-Engineers GmbH

In der folgenden Liste finden Sie aller bisher veröffentlichten Stände unserer Technischen und Organisatorischen Maßnahmen (TOMs) als PDF-Download:

| Version, Veröffentlichungsdatum | Download als PDF |
|---|---|
| **aktuell: 1.0 vom 7.5.2018** | **ITEG-TOMs_1.0_vom_2018-05-07.pdf** |

## Ausfüll-Hilfen

Dieses Kapitel bietet ein paar "Ausfüllhilfen" zur Vervollständigung des ITEG-Musters oder einer anderen ähnlichen Vorlage.

Bei Verwendung fremder Muster beachten Sie bitte unsere "Änderungen zur WKO-Vorlage" im nächsten Kapitel.

### Vertragspartner

Bei den Vertragspartnern bevorzugen wir die DSGVO-Begriffe "**Verantwortlicher**" und "**Auftragsverarbeiter**" über die Wirtschafts-Begriffe "Auftraggeber" und "Auftragnehmer".

Die Kontaktdaten von ITEG finden Sie unter iteg.at/kontakt.

### Kontakt für Informationsanfragen von potentiell betroffenen Personen

Wir müssen darauf bestehen bei den Daten des Verantwortlichen oder in einem eigenen Satz unbedingt einen **Kontakt (E-Mail-Adresse und Telefonnummer) anzugeben an die wir Informationsanfragen von potentiell betroffenen Personen weiterleiten können**.

### Gegenstand der Vereinbarung

Die Branchen-typische Überbegriffe, passend für Kap. 1. (1), sind:

| Überbegriff | Kurzbeschreibung |
|---|---|

| | |
|---|---|
| "Shared Hosting" bzw. "Webhosting" bzw. "LAMP-Hosting" | Hosting von Webauftritten und zugehörigen Datenbanken auf Shared-Hosting-Servern.<br>Auf einem Shared-Hosting-Server werden meist Webauftritte verschiedener Kunden parallel gehostet.<br>Die Bereiche der verschiedenen Kunden werden so gut wie mit vertretbarem Aufwand untereinander getrennt,<br>aber ein Rest-Risiko von "local privilege escalations" besteht immer.<br>Administrativen Zugriff auf den ganzen Server haben nur die Administratoren von ITEG. |
| "Mail-Hosting" | Hosting von E-Mail-Postfächern und/oder Weiterleitungs-E-Mail-Adressen |
| "Root-Hosting" | Beim Root-Hosting steht ein ganzer virtueller Linux-Server einem Hosting-Kunden (und dessen Web-Agenturen) exklusiv zur Verfügung.<br>Dabei hat auch der Hosting-Kunden administrativen Zugriff auf den ganzen virtuellen Server. |
| "Domain-Hosting" bzw. "DNS-Hosting" | Neben dem Betrieb des DNS (Domain-Name-Servers) umfasst das üblicherweise auch die Verwaltung der Inhaber-Daten der Domain beim jeweiligen Registrar, also bei der für Domainvergabe authorisierten Stelle. |

### Datenkategorien

Für die Kategorien der verarbeiteten Daten für Kap. 1. (2) gibt es verschiedene Ansätze.

Hier einige Beispiele:

| Begriff | Anmerkungen |
|---|---|
| Personenstammdaten | Im Zweifel sollten Details angegeben werden, z.B. Adresse, E-Mail-Adresse, Kontonummern, Bonitätsdaten, ...<br>Manche Daten unterliegen besonderem Schutz, z.B. Religionsbekenntnis, Ethnische Herkunft, Strafregisterauszug |
| Kommunikationsdaten | z.B. E-Mails, laut "Erwägung 30" auch IP-Adressen (in Log-Files auch von Web-Servern) |
| Vertragsdaten | Angebote, Bestellungen, Aufträge, Lieferscheine, ... |
| Protokolldaten | ... |

Anmerkung: Wichtige Log-Dateien (inkl. IP-Adressen) werden bei ITEG üblicherweise 6 Monate aufbewahrt was wir als angemessen und für Nachforschungen notwendig erachten.

### Personenkategorien

Bei den Kategorien der betroffenen Personen für Kap. 1. (3) kann bzw. muss man relativ großzügig pauschalisieren.

Z.B.: Kunden, Interessenten, Lieferanten, Mitarbeiter.

Die Unterscheidung zwischen privatpersonen und Firmen ist insbesondere in Österreich relativ sinnlos (Personen-Definition im Verfassung), aber auch international wird man kaum Daten einer Firma verarbeiten ohne dass zumindest die Kontaktdaten (Name, Telefonnummer, E-Mail-Adresse) einer natürlichen Ansprechperson enthalten sind.

### Sub-Auftragsverarbeiter bzw. Sub-Auftragnehmer

ITEG greift zur Datenverarbeitung auf keinerlei Sub-Auftragsverarbeiter zurück.

Das CityNet Hall als Anbieter bzw. Sub-Auftragnehmer für Serverhousing hat zwar physischen Zugriff auf unsere Server und könnte theoretisch Festplatten "rauben", darf dies aber nicht und ist selbst mehrfach ISO-zertifiziert (ISO-27001, ISO-9001). Der Zugang zum Data-Center ist ausserdem mit 2 Zugagnschips und PIN abgesichert und das ganze Data-Center ist Video-überwacht.
Wir betrachten die Tätigkeit des CityNets als Rackspace-Vermieter und Access-Lieferant (Carrier) daher nicht als Sub-Auftragsverarbeitung.

### Technische und Organisatorische Maßnahmen (TOMs)

ITEG ist seit 18.12.2018 von CIS nach ISO-27001 zertifiziert, was um eine DImension besser ist als alle TOM-Listen die sich in Mustern für Auftragsvereitungs-Vereinbarungen finden.

Wir bitten daher entweder auf unsere ISO-Zertifizierung oder auf unsere eigene Liste der Technischen und Organisatorischen Maßnahmen (TOMs) zurück zugreifen bzw. zu verweisen, siehe Download-Liste ganz oben auf dieser Seite.
Aktuell ist Version 1.0 vom 7.5.2018: ITEG-TOMs_1.0_vom_2018-05-07.pdf

## Änderungen gegenüber Wirtschaftskammer-Vorlage und Anmerkungen

Falls Sie sich mit dem Muster der WKO schon beschäftigt haben oder als Kunde eine selbst formulierte Auftragsverarbeitungs-Vereinbarung evtl. auf dieser Basis schreiben möchten bitten wir um Beachtung folgender **erforderlicher Änderungen** gegenüber dem WKO-Muster.

Bitte beachten Sie grundsätzlich auch die Ausfüllhilfen weiter oben.

## Auftragsverarbeiter statt Auftragnehmer, Verantwortlicher statt Auftragggeber

Bitte, Danke.

## Änderung bei "3. Pflichten des Auftragsverarbeiters" Ziffer (3), ITEG-TOMs statt Anhang 1

**Kein Verweis auf "*Anhang 1*"** (siehe unten) **sondern:**

---

Einzeilheiten sind ITEG's Technischen und Organisatorischen Maßnahmen in der zum Zeitpunkt der Vereinbarung gültigen Version 1.0 vom 7.5.2018 zu entnehmen (siehe https://iteg.at/TOMs).

---

## Einschränkung zu "3. Pflichten des Auftragsverarbeiters" Ziffer (4), "im Rahmen seiner Zuständigkeit"

Die einzigen Maßnahmen die ITEG im Sinne dieser Ziffer setzen kann sind das sicherstellen einer normalen Server-Verfügbarkeit und die Erreichbarkeit für irrtümlich an ITEG gestellte Informationsanfragen von potentiell betroffenen Personen.

Daher möglichst im ersten Satz statt "*Der Auftragsverarbeiter ergreift die technischen ...*" erweitert "Der Auftragsverarbeiter ergreift im Rahmen seiner Zuständigkeit die technischen ..."

## Anmerkung zu "3. Pflichten des Auftragsverarbeiters" Ziffer (6)

Bezüglich der Auftragsverarbeitungen beschränkt sich das Verarbeitungsverzeichnis auf die in Kapitel 1. der einzelnen Vereinbarungen genannten Rahmeninformationen pro Hosting-Kunde.

## Milderung "3. Pflichten des Auftragsverarbeiters" Ziffer (7), Stichproben statt jederzeit, sowie Hinweis Voranmeldung

Eine "*jederzeitiger Einsichtnahme und Kontrolle ... der Datenverarbeitungseinrichtungen*" ist weder organisatorisch noch rechtlich möglich.

Auf ausdrücklichen Wunsch kann nach Voranmeldung (auch beim Betreiber des Data-Centers) eine Besichtigung des Data-Centers organisiert werden.

**Daher**: "*jederzeitiger Einsichtnahme*" **durch** "zur stichprobenartigen Einsichtnahme" **ersetzen**.

Weiters bitte anhängen:

---

Einsichtnahmen sind nur nach Voranmeldung und mit Zustimmung des Betreibers des Datacenters möglich.

---

## Kürzung "3. Pflichten des Auftragsverarbeiters" Ziffer (8)

Die Variante "*/ in dessen Auftrag zu vernichten [1]*" ist **zu streichen**.

Der Satz mit "*speziellen technischen Format*" ist irrelevant und kann gestrichen werden.

## Streichung bzw. Kürzung "5. Sub-Auftragsverarbeiter"

Da wir den Housing-Anbieter (Rackspace- und Access-Anbieter) nicht als Auftragsverarbetier sehen gibt es seitens ITEG keine Sub-Auftragsverarbeiter. Siehe dazu auch in der Ausfüllhilfe weiter oben und unser Muster.

Daher kann Kapitel 5 weggelassen oder durch den Satz aus unserem ersetzt oder ergänzt werden.

## Zusätzliches Kapitel "6. Pflichten des Verantwortlichen" bzw. Auftraggebers

Alle bisherigen Security-Incidents bei ITEG hatten Ihren Ursprung in mangelhafter Qualität bzw. Wartung der vom Hosting-Kunden eingesetzten Software, z.B. in unsicheren WordPress-Plugins, ungeschützten Administrations-Zugängen von J2EE-Frameworks, unsicherer Programmierung seitens der individuellen Web-Entwickler, u.ä.

Daher möchten wir folgende Kundenpflicht in Auftragsverarbeitungs-Vereinbarungen aufnehmen (z.B. als Kap. 6, siehe unser Muster):

---

Der Verarbeiter bzw. Auftraggeber ist verpflichtet

- Zugangsdaten zu ITEG-Systemen (Webspace, Mailboxen, u.ä.) geheim zu halten bzw. nur soweit unbedingt nötig an IT-Betreuer bzw. Web-Designer bzw. Web-Entwickler weiterzugeben.
  Unter Zugangsdaten fallen von ITEG vergebene Passwörter sowie von ITEG eingetragene Kunden-eigene private SSH-Keys.
- den Verlust solcher Zugangsdaten zu ITEG-Systemen sowie etwaige Hacks eines bei ITEG gehosteten eigenen Web-Auftritts umgehend an ITEG zu melden

---

## Zusätzliche Kapitelüberschrift "7. Unterschriften"

Nur zur klaren Trennung vom vorigen Kapitel.

## Ersatz für "Anlage 1", Technische und Organisatorische Maßnahmen (TOMs)

Die Schlagwort-Liste im WKO-Muster passt nicht auf Hosting bzw. auf ITEG als hochspezialisiertem KMU.

Stattdessen muss in Kap. 3. Ziffer (3) auf ITEG's Technischen und Organisatorischen Maßnahmen (TOMs) verwiesen werden, vgl. unseren Formulierungsvorschlag weiter oben.
Aktuelle Version unserer TOMs ist Version 1.0 vom 7.5.2018: ITEG-TOMs_1.0_vom_2018-05-07.pdf.